IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for preventing an outbreak of malicious code, comprising:

a) identifying malicious code at a local location on a network;

b) encrypting information relating to the malicious code at the local location;

c) sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network; and

d) blocking instances of the malicious code at the remote locations for a predetermined amount of time based on the information;

e) registering at least one of a name and checksum of a file containing the malicious code as a known threat;

[e)]f) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the malicious code;

[f)]g) wherein the information relating to the malicious code includes an identification of the source of the malicious code, wherein communications originating at the identified source are denied access to the remote locations for the predetermined amount of time.

2. (Original) The method as recited in claim 1, wherein the malicious code is at least one of a virus, worm, and Trojan.

3. (Cancelled)

4. (Cancelled)

5. (Original) The method as recited in claim 1, further comprising executing countermeasures for limiting the effect of the malicious code at the local location.

6. (Cancelled)

7. (Original) The method as recited in claim 1, wherein additional information about the malicious code is retrieved if an aspect of the malicious code is not recognized.

8. (Currently Amended) A computer program product for managing an outbreak of malicious code, comprising:

a) computer code for identifying malicious code at a local location on a network;

b) computer code for encrypting information relating to the malicious code at the local location;

c) computer code for sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network; and

d) computer code for blocking instances of the malicious code at the remote locations for a predetermined amount of time based on the information;

e) computer code for registering at least one of a name and checksum of a file containing the malicious code as a known threat;

[e)]f) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the malicious code;

[f)]g) wherein the information relating to the malicious code includes an identification of the source of the malicious code, wherein communications originating at the identified source are denied access to the remote locations for the predetermined amount of time.

9. (Currently Amended) A system for preventing an outbreak of malicious code, comprising:

a) logic for identifying malicious code at a local location on a network;

b) logic for encrypting information relating to the malicious code at the local location;

c) logic for sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network; and

d) logic for blocking instances of the malicious code at the remote locations for a predetermined amount of time based on the information;

e) logic for registering at least one of a name and checksum of a file containing the malicious code as a known threat;

[e)]f) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the malicious code;

[f)]g) wherein the information relating to the malicious code includes an identification of the source of the malicious code, wherein communications originating at the identified source are denied access to the remote locations for the predetermined amount of time.

10.-18. (Cancelled)

19. (Currently Amended) A method for denying access to a hacker, comprising:

a) identifying an attack by a hacker at a local location on a network;

b) encrypting information relating to the attack at the local location;

c) sending the encrypted information relating to the attack to a plurality of remote locations utilizing the network; and

d) restricting access to the remote locations for a predetermined amount of time based on the information;

e) registering at least one of a name and checksum of a file associated with the attack as a known threat;

[e)]f) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the attack;

[f)]g) wherein the information relating to the attack includes an identification of the source of the attack, wherein communications originating at the identified source are denied access to the remote locations for the predetermined amount of time.

20. (Original) The method as recited in claim 19, wherein the attack attempts to create a denial of service.

21. (Cancelled)

22. (Previously Presented) The method as recited in claim 19, further comprising registering the source of the attack as a known threat.

23. (Original) The method as recited in claim 19, wherein the attack is recognized based at least in part on recognizing that the source of the attack is registered as a known threat.

24. (Original) The method as recited in claim 19, further comprising executing countermeasures for limiting the effect of the attack at the local location.

25. (Original) The method as recited in claim 19, wherein additional information about the attack is retrieved if an aspect of the attack is not recognized.

26. (Currently Amended) A computer program product for denying access to a hacker, comprising:

a) computer code for identifying an attack by a hacker at a local location on a network;

b) computer code for encrypting information relating to the attack at the local location;

c) computer code for sending the encrypted information relating to the attack to a plurality of remote locations utilizing the network; and

d) computer code for restricting access to the remote locations for a predetermined amount of time based on the information;

e) computer code for registering at least one of a name and checksum of a file associated with the attack as a known threat;

[e)]f) ~~for~~ wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the attack;

[f)]g) wherein the information relating to the attack includes an identification of the source of the attack, wherein communications originating at the identified source are denied access to the remote locations for the predetermined amount of time.

27. (Currently Amended) A system for denying access to a hacker, comprising:

a) logic for identifying an attack by a hacker at a local location on a network;

b) logic for encrypting information relating to the attack at the local location;

c) logic for sending the encrypted information relating to the attack to a plurality of remote locations utilizing the network; and

d) logic for restricting access to the remote locations for a predetermined amount of time based on the information;

e) logic for registering at least one of a name and checksum of a file associated with the attack as a known threat;

[e)]f) wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the attack;

[f)]g) wherein the information relating to the attack includes an identification of the source of the attack, wherein communications originating at the identified source are denied access to the remote locations for the predetermined amount of time.

28.-36. (Cancelled)

37. (Previously Presented) A method for preventing an outbreak of malicious code, comprising:

a) identifying malicious code at a local location on a network;

b) wherein the malicious code is at least one of a virus, worm and, Trojan;

c) wherein the malicious code is recognized based at least in part on recognizing that at least one of a checksum and a file name of the malicious code is registered as a known threat;

d) encrypting information relating to the malicious code at the local location, wherein the information is selected from the group consisting of a type, context, protocol, severity, reporting server, and IP address associated with the malicious code, and wherein the information relating to the attack includes an identification of the source of the attack, wherein communications originating at the identified source are denied access to the remote locations for the predetermined amount of time;

e) sending the encrypted information relating to the malicious code to a plurality of remote locations utilizing the network;

f) restricting access to the remote locations by communications originating at the source of the malicious code for a predetermined amount of time based on the information;

g) executing countermeasures for limiting the effect of the malicious code at the local location; and

h) retrieving additional information about the malicious code if an aspect of the attack is not recognized.

38. (Previously Presented) The method as recited in claim 1, wherein the information includes a type, context, protocol, severity, reporting server, and IP address associated with the malicious code.

39. (Previously Presented) The method as recited in claim 38, wherein the type is selected from the group consisting of an unwanted message attempt, and a denial of service attack.

40. (Previously Presented) The method as recited in claim 38, wherein the context is selected from the group consisting of a virus name, a subject, a mail header, and a magic number for a message.

41. (Previously Presented) The method as recited in claim 1, further comprising attempting to identify a source of the malicious code, and, if the source is identified, retrieving information about the source from a database.

42. (Previously Presented) The method as recited in claim 1, wherein additional information relating to the malicious code is retrieved from a database if the malicious code is not identified in conjunction with an event at the local location on the network.

43. (New) The method of claim 1, wherein a simple mail transfer protocol (SMTP) is utilized for collecting the information that is associated with spam attempts, spam-relay attempts, denial of service (DoS) attacks, and malicious attachment forwarding; a net news transfer protocol (NNTP) is utilized for collecting the information that is associated with DoS attacks, malicious attachment

forwarding, and cross-posting; a file transfer protocol (FTP) is utilized for collecting the information that is associated with DoS attacks, and repeated unsuccessful logins; a hypertext transfer protocol (HTTP) is utilized for collecting the information that is associated with malicious content, DoS attacks, and known hacking attempts; and a firewall protocol is utilized for collecting the information that is associated with intrusion detection, and port scanning attempts.